JP01/772
EU

02.02.01

#4

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年　８月　２日

出願番号
Application Number: 特願２０００－２３４７４１

出願人
Applicant (s): ソニー株式会社

09/937797

２００１年　３月　２日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２００１－３０１５１６４

【書類名】　特許願

【整理番号】　0000171303

【提出日】　平成12年 8月 2日

【あて先】　特許庁長官殿

【国際特許分類】　G06F 17/60

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　金巻　裕史

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　佐竹　清

【特許出願人】

【識別番号】　000002185

【氏名又は名称】　ソニー株式会社

【代表者】　出井　伸之

【代理人】

【識別番号】　100094053

【弁理士】

【氏名又は名称】　佐藤　隆久

【手数料の表示】

【予納台帳番号】　014890

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9707389

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　通信制御装置、通信システムおよびその方法

【特許請求の範囲】

【請求項１】

単数または複数の第１の通信装置からの要求に応じてネットワーク上の第２の通信装置で処理を行うことに関しての通信を制御する通信制御装置であって、

前記第１の通信装置を識別するための装置識別情報を記憶する記憶手段と、

前記第１の通信装置からの要求に応じて、当該第１の通信装置に対応する前記装置識別情報を含む要求を前記第２の通信装置に送信する送信手段と、

前記要求の送信元の装置を識別するための装置識別情報を含む応答を前記第２の通信装置から受信する受信手段と、

前記応答に含まれる前記装置識別情報と前記記憶手段に記憶された前記装置識別情報とが一致するか否かに基づいて、前記受信した応答に対応した前記要求が、前記記憶手段に前記装置識別情報が記憶されている正当な前記第１の通信装置によるものであるかを判断する制御手段と

を有する通信制御装置。

【請求項２】

前記制御手段は、

前記応答に含まれる前記装置識別情報と前記記憶手段に記憶された前記装置識別情報とが一致しない場合に、前記第２の通信装置に所定の通知を行う

請求項１に記載の通信制御装置。

【請求項３】

前記制御手段は、

前記応答に含まれる装置識別情報と前記記憶手段に記憶された前記装置識別情報とが一致しない場合に、前記応答に含まれる処理の結果が用いられる取り引き先の装置に所定の通知を行う

請求項１に記載の通信制御装置。

【請求項４】

前記送信手段は、

前記第１の通信装置から受信した利用者識別情報と、当該第１の通信装置に対応する前記装置識別情報とを含む前記要求を前記第２の通信装置に送信する

請求項１に記載の通信制御装置。

【請求項５】

前記記憶手段は、

前記第１の通信装置から受信した前記装置識別情報を記憶する

請求項１に記載の通信制御装置。

【請求項６】

前記記憶手段は、

当該通信制御装置の電源が投入されたときに前記第１の通信装置から受信した前記装置識別情報を記憶する

請求項５に記載の通信制御装置。

【請求項７】

前記制御手段は、

前記第１の通信装置と前記第２の通信装置との間の通信履歴を前記記憶手段に書き込む

請求項１に記載の通信制御装置。

【請求項８】

前記制御手段は、

前記応答に含まれる前記第２の通信装置の処理結果を、前記要求の送信元の前記第１の通信装置に送信する

請求項１に記載の通信制御装置。

【請求項９】

前記制御手段は、

前記受信手段から受信した情報に応じて、待機状態にある前記第１の通信装置が動作状態になるように制御する

請求項１に記載の通信制御装置。

【請求項１０】

前記制御手段は、

前記第１の通信装置が接続されたネットワークと、前記第２の通信装置が接続されたネットワークとの間の通信を制御する

請求項１に記載の通信制御装置。

【請求項１１】

前記制御手段は、

ゲートウェイとしての処理を行う

請求項１０に記載の通信制御装置。

【請求項１２】

前記装置識別情報は、前記第１の通信装置の製造元で付された当該通信装置を一意に識別可能な識別子である

請求項１に記載の通信制御装置。

【請求項１３】

前記利用者識別情報は、登録した利用者に予め割り当てられた識別子である

請求項４に記載の通信制御装置。

【請求項１４】

前記受信手段は、

前記第２の通信装置が行った認証処理の結果を含む前記応答を前記第２の通信装置から受信する

請求項１に記載の通信制御装置。

【請求項１５】

単数または複数の第１の通信装置からの要求に応じてネットワーク上の第２の通信装置で処理を行うこと関する通信を通信制御装置で制御する通信システムであって、

前記通信制御装置は、

前記第１の通信装置を識別するための装置識別情報を記憶する第１の記憶手段と、

前記第１の通信装置からの要求に応じて、当該第１の通信装置に対応する前記装置識別情報と利用者識別情報とを含む要求を前記第２の通信装置に送信する第１の送信手段と、

前記要求の送信元の装置を識別するための装置識別情報を含む応答を前記第２の通信装置から受信する第１の受信手段と、

前記応答に含まれる前記装置識別情報と前記第１の記憶手段に記憶された前記装置識別情報とが一致するか否かに基づいて、前記受信した応答に対応した前記要求が、前記第１の記憶手段に前記装置識別情報が記憶されている正当な前記第１の通信装置によるものであるかを判断する制御手段と

を有し、

前記第２の通信装置は、

前記要求を受信する第２の受信手段と、

前記利用者識別情報と処理結果を送信する送信先の情報とを対応付けて記憶する第２の記憶手段と、

前記要求に応じて所定の処理を行う処理手段と、

前記要求に含まれる前記利用者識別情報に対応する前記送信先の情報を前記第２の記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記処理の結果と前記要求に含まれる前記装置識別情報とを対応付けて送信する第２の送信手段と

を有する

通信システム。

【請求項１６】

単数または複数の第１の通信装置からの要求に応じてネットワーク上の第２の通信装置で処理を行うことに関する通信を通信制御装置で制御する通信方法であって、

前記第１の通信装置から前記通信制御装置に出された要求に応じて、当該第１の通信装置に対応する装置識別情報と利用者識別情報とを含む要求を前記通信制御装置から前記第２の通信装置に送信し、

前記第２の通信装置において、受信した前記要求に応じた所定の処理を行い、

前記第２の通信装置において、前記要求に含まれる前記利用者識別情報に対応する送信先の情報に基づいて、前記処理の結果と前記要求に含まれる前記装置識別情報とを含む応答を前記通信制御装置に送信し、

前記通信制御装置において、受信した前記応答に含まれる前記装置識別情報と、予め保持した前記第１の通信装置の前記装置識別情報とが一致するか否かに基づいて、前記受信した応答に対応した前記要求が、正当な前記第１の通信装置によるものであるかを判断する

通信方法。

【請求項１７】

前記通信制御装置は、

前記応答に含まれる前記装置識別情報と予め保持した前記第１の通信装置の前記装置識別情報とが一致しない場合に、前記第２の通信装置に所定の通知を行う

請求項１６に記載の通信方法。

【請求項１８】

前記通信制御装置は、

前記応答に含まれる前記装置識別情報と予め保持した前記第１の通信装置の前記装置識別情報とが一致しない場合に、前記応答に含まれる処理の結果が用いられる取り引き先の装置に所定の通知を行う

請求項１６に記載の通信方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、例えば電子商取引情報を認証などの処理を行う際用いられる通信制御装置、通信システムおよびその方法に関する。

【０００２】

【従来の技術】

インターネットなどのネットワークを介して商品等の販売や代金の決済を行う電子商取引が普及している。

このような電子商取引を用いて利用者が商品等を購入する場合には、例えば、利用者が店舗や各家庭に設置されたパーソナルコンピュータなどの発注者端末装置を操作して、ネットワークを介して、商品等の販売を行うサーバ装置にアクセスを行う。これにより、サーバ装置から発注者端末装置に商品の写真、特性およ

び価格などの情報が提供され、発注者端末装置のディスプレイに表示される。利用者は、このような情報を見ながら、購入を希望する商品等を選択し、選択した商品等の発注処理を行う。発注処理は、利用者個人を特定する個人ＩＤ情報、発注する商品等を指定した情報およびその決済方法等の情報を、発注者端末装置を操作して入力し、これをネットワークを介してサーバ装置に送信する。

【０００３】

このような電子商取引では、ネットワーク銀行などが、ネットワークを介した取り引きに関しての決済業務を行うが、当該決済を行うに当たって、決済対象となる電子商取引の内容の正当性が認証されている必要がある。

従って、電子商取引では、このような電子商取引の内容の正当性を認証する処理を行う認証装置が用いられる。当該認証装置を用いた認証業務は、ネットワーク銀行、あるいは他の信頼性のある機関が行う。

【０００４】

【発明が解決しようとする課題】

ところで、上述したような認証装置では、例えば、個人ＩＤ情報を他人が不正に取得した場合に、当該他人は、その個人ＩＤ情報を用いて、認証装置に対して認証要求を出すことができ、不正な取り引きが行われてしまう可能性があるという問題がある。

また、家庭内に複数の端末装置を設けた場合に、外部のネットワークを介して行われる電子商取引やセキュリティに関する機能を端末装置毎に持たせると、効率が悪いと共に、例えば家庭単位で通信履歴を管理するときに不便である。

【０００５】

本発明は上述した従来技術の問題点に鑑みてなされ、不正に取得した他人の個人ＩＤ情報に基づいて不正な認証手続が行われることを回避する通信制御装置、通信システムおよびその方法を提供することを目的とする。

また、本発明は、複数の端末装置を用いてネットワークを介した電子商取引などを行う場合に、当該電子商取引に必要な機能の割り当て、並びに通信履歴の管理を効率的に行うことができる通信制御装置、通信システムおよびその方法を提供することを目的とする。

【０００６】

【課題を解決するための手段】

上述した従来技術の問題点を解決し、上述した目的を達成するために、第１の発明の通信制御装置は、単数または複数の第１の通信装置からの要求に応じてネットワーク上の第２の通信装置で処理を行うことに関しての通信を制御する通信制御装置であって、前記第１の通信装置を識別するための装置識別情報を記憶する記憶手段と、前記第１の通信装置からの要求に応じて、当該第１の通信装置に対応する前記装置識別情報を含む要求を前記第２の通信装置に送信する送信手段と、前記要求の送信元の装置を識別するための装置識別情報を含む応答を前記第２の通信装置から受信する受信手段と、前記応答に含まれる前記装置識別情報と前記記憶手段に記憶された前記装置識別情報とが一致するか否かに基づいて、前記受信した応答に対応した前記要求が、前記記憶手段に前記装置識別情報が記憶されている正当な前記第１の通信装置によるものであるかを判断する制御手段とを有する。

【０００７】

第１の発明の通信制御装置の作用は以下のようになる。

送信手段、第１の通信装置からの要求に応じて、当該第１の通信装置に対応する前記装置識別情報を含む要求を第２の通信装置に送信する。

そして、受信手段が、前記要求の送信元の装置を識別するための装置識別情報を含む応答を前記第２の通信装置から受信する。

次に、制御手段によって、前記受信した応答に含まれる前記装置識別情報と記憶手段に記憶された前記装置識別情報とが一致するか否かに基づいて、前記受信した応答に対応した前記要求が、前記記憶手段に前記装置識別情報が記憶されている正当な前記第１の通信装置によるものであるかを判断する。

【０００８】

また、第１の発明の通信制御装置は、好ましくは、前記制御手段は、前記応答に含まれる前記装置識別情報と前記記憶手段に記憶された前記装置識別情報とが一致しない場合に、前記第２の通信装置に所定の通知を行う。

【０００９】

また、第１の発明の通信制御装置は、好ましくは、前記制御手段は、前記応答に含まれる装置識別情報と前記記憶手段に記憶された前記装置識別情報とが一致しない場合に、前記応答に含まれる処理の結果が用いられる取り引き先の装置に所定の通知を行う。

【００１０】

また、第１の発明の通信制御装置は、好ましくは、前記送信手段は、前記第１の通信装置から受信した利用者識別情報と、当該第１の通信装置に対応する前記装置識別情報とを含む前記要求を前記第２の通信装置に送信する。

【００１１】

また、第１の発明の通信制御装置は、好ましくは、前記記憶手段は、前記第１の通信装置から受信した前記装置識別情報を記憶する。

【００１２】

また、第１の発明の通信制御装置は、好ましくは、前記記憶手段は、当該通信制御装置の電源が投入されたときに前記第１の通信装置から受信した前記装置識別情報を記憶する。

【００１３】

また、第１の発明の通信制御装置は、好ましくは、前記制御手段は、前記第１の通信装置と前記第２の通信装置との間の通信履歴を前記記憶手段に書き込む。

【００１４】

また、第１の発明の通信制御装置は、好ましくは、前記制御手段は、前記応答に含まれる前記第２の通信装置の処理結果を、前記要求の送信元の前記第１の通信装置に送信する。

【００１５】

また、第１の発明の通信制御装置は、好ましくは、前記制御手段は、前記受信手段から受信した情報に応じて、待機状態にある前記第１の通信装置が動作状態になるように制御する。

【００１６】

また、第１の発明の通信制御装置は、好ましくは、前記制御手段は、前記第１の通信装置が接続されたネットワークと、前記第２の通信装置が接続されたネッ

トワークとの間の通信を制御する。

【００１７】

また、第１の発明の通信制御装置は、好ましくは、前記装置識別情報は、前記第１の通信装置の製造元で付された当該通信装置を一意に識別可能な識別子である。

【００１８】

また、第１の発明の通信制御装置は、好ましくは、前記利用者識別情報は、登録した利用者に予め割り当てられた識別子である

請求項１に記載の通信制御装置。

【００１９】

また、第２の発明の通信システムは、単数または複数の第１の通信装置からの要求に応じてネットワーク上の第２の通信装置で処理を行うこと関する通信を通信制御装置で制御する通信システムであって、前記通信制御装置は、前記第１の通信装置を識別するための装置識別情報を記憶する第１の記憶手段と、前記第１の通信装置からの要求に応じて、当該第１の通信装置に対応する前記装置識別情報と利用者識別情報とを含む要求を前記第２の通信装置に送信する第１の送信手段と、前記要求の送信元の装置を識別するための装置識別情報を含む応答を前記第２の通信装置から受信する第１の受信手段と、前記応答に含まれる前記装置識別情報と前記第１の記憶手段に記憶された前記装置識別情報とが一致するか否かに基づいて、前記受信した応答に対応した前記要求が、前記第１の記憶手段に前記装置識別情報が記憶されている正当な前記第１の通信装置によるものであるかを判断する制御手段とを有し、前記第２の通信装置は、前記要求を受信する第２の受信手段と、前記利用者識別情報と処理結果を送信する送信先の情報とを対応付けて記憶する第２の記憶手段と、前記要求に応じて所定の処理を行う処理手段と、前記要求に含まれる前記利用者識別情報に対応する前記送信先の情報を前記第２の記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記処理の結果と前記要求に含まれる前記装置識別情報とを対応付けて送信する第２の送信手段とを有する。

【００２０】

また、第３の発明の通信方法は、単数または複数の第１の通信装置からの要求に応じてネットワーク上の第２の通信装置で処理を行うことに関する通信を通信制御装置で制御する通信方法であって、前記第１の通信装置から前記通信制御装置に出された要求に応じて、当該第１の通信装置に対応する装置識別情報と利用者識別情報とを含む要求を前記通信制御装置から前記第２の通信装置に送信し、前記第２の通信装置において、受信した前記要求に応じた所定の処理を行い、前記第２の通信装置において、前記要求に含まれる前記利用者識別情報に対応する送信先の情報に基づいて、前記処理の結果と前記要求に含まれる前記装置識別情報とを含む応答を前記通信制御装置に送信し、前記通信制御装置において、受信した前記応答に含まれる前記装置識別情報と、予め保持した前記第１の通信装置の前記装置識別情報とが一致するか否かに基づいて、前記受信した応答に対応した前記要求が、正当な前記第１の通信装置によるものであるかを判断する。

【００２１】

【発明の実施の形態】

以下、本発明の実施形態に係わるトランザクション認証システムについて説明する。

図１は、本実施形態のトランザクション認証システム１０１の全体構成図である。

図１に示すように、トランザクション認証システム１０１では、例えば、発注者３１の発注者端末装置１１と、受注者３３の受注者端末装置１５と、ネットワーク銀行４０の認証装置５０とが、インターネットなどの外部ネットワーク（通信網）９を介して接続されており、発注者３１と受注者３３との間のトランザクション（取り引き）の正当性を認証装置５０で認証する。

なお、当該ネットワークに接続されているホームネットワークシステム（発注者端末システム）１０および受注者端末装置１５の数は任意である。

【００２２】

本実施形態では、ホームネットワークシステム１０が本発明の通信制御装置に対応し、端末装置11_1～11_4が本発明の第１の通信装置に対応し、認証装置５０が本発明の第２の通信装置に対応している。

【００２３】

本実施形態では、例えば、発注者３１および受注者３３とネットワーク銀行４０との間で認証を行うことに関しての契約が成されている。また、発注者３１と引き落とし銀行４２との間では、例えば、ネットワーク銀行４０によって認証された取り引きに関しての引き落としを行う旨の契約がなされている。また、ネットワーク銀行４０と保険会社４３との間では、ネットワーク銀行４０が係わった電子商取引によって生じた損害についての保険契約がなされている。

【００２４】

以下、トランザクション認証システム１０１を構成する各装置について説明する。

〔ホームネットワークシステム１０〕

図１および図２に示すように、ホームネットワークシステム１０は、発注者３１の各家庭などに構築されており、ホームネットワークシステム１０のホームゲートウェイ１２が、図１に示す受注者端末装置１５および認証装置５０が接続される外部ネットワーク９に有線あるいは無線で接続されている。

また、ホームゲートウェイ１２には、例えば、家庭内の内部ネットワーク１３を介して、端末装置11_1，11_2，11_3，11_4が有線あるいは無線で接続される。

端末装置11_1～11_4は、例えば、デジタルテレビ受信装置、パーソナルコンピュータ、電話機およびゲーム機などである。

端末装置11_1～11_4の各々には、例えば製造元で当該端末装置を識別するための装置ＩＤ情報が割り当てられており、当該装置ＩＤ情報が各端末装置の内部メモリに記憶されている。例えば、端末装置11_1には装置ＩＤ情報ID_{M1}が割り当てられ、端末装置11_2には装置ＩＤ情報ID_{M2}が割り当てられ、端末装置11_3には装置ＩＤ情報ID_{M3}が割り当てられ、端末装置11_4には装置ＩＤ情報ID_{M4}が割り当てられている。

【００２５】

図３は、ホームゲートウェイ１２の構成図である。

ホームゲートウェイ１２は、例えば、外部ネットワークＩ／Ｆ６１、内部ネッ

トワークＩ／Ｆ６２、暗号化部６３、復号部６４、記憶部６５、制御部６６および署名検証部６７を有する。

ここで、外部ネットワークＩ／Ｆ６１および内部ネットワークＩ／Ｆ６２が、第１の発明の送信手段および受信手段、並びに第２の発明の第１の送信手段および第２の受信手段に対応している。また、記憶部６５が、第１の発明の記憶手段および第２の発明の第１の記憶手段に対応している。また、制御部６６が第１の発明および第２の発明の制御手段に対応している。

【００２６】

外部ネットワークＩ／Ｆ６１は、外部ネットワーク９を介して認証装置５０との間で、情報あるいは要求の送受信を行なう。

内部ネットワークＩ／Ｆ６２は、内部ネットワーク１３を介して端末装置11_1～11_4との間で、情報あるいは要求の送受信を行なう。

暗号化部６３は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部６４は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部６５は、例えば、ホームゲートウェイ１２の電源が投入されたときに電源がオンになっている端末装置11_1～11_4から内部ネットワーク１３を介して受信した装置ＩＤ情報ID_{M1}～ID_{M4}を記憶している。

また、記憶部６５は、発注者３１が作成した秘密鍵$K_{31,S}$などを格納する。

署名検証部６７は、例えば、認証装置５０が作成した署名情報を、ネットワーク銀行４０の公開鍵$K_{40,P}$を用いて検証する。

制御部６６は、発注者端末装置１１内の各構成要素の処理を統括的に制御する。

制御部６６は、ホームゲートウェイ１２を介した端末装置11_1～11_4と認証装置５０との間の通信の履歴を示す履歴情報を生成し、これを記憶部６５に記憶する。

そのため、記憶部６５に記憶された履歴情報にアクセスを行うだけで、家庭内に設けられた端末装置11_1～11_4を用いた通信の履歴を簡単に知ることができ、管理が容易になる。

【００２７】

また、制御部６６は、例えば、待機状態（スタンバイ状態）になっている端末装置11_1～11_4に対してのアクセスを、外部ネットワーク９を介して受けた場合に、対応する端末装置11_1～11_4が動作状態になるように制御する。

【００２８】

制御部６６は、例えば、発注者３１による操作に応じて端末装置11_1～11_4から内部ネットワークＩ／Ｆ６２が受信した、発注情報ａ１と、個人キー情報ｋ１と（本発明の利用者識別情報）、個人ＩＤ情報ＩＤ１（本発明の利用者識別情報）と、装置ＩＤ情報ID_{M1}～ID_{M4}（本発明の装置識別情報）との全体に対してを暗号化を行い、もしくは個別情報毎に暗号化を行い、当該暗号化した情報を格納した認証要求Ｉｎｆ１を生成する。

また、制御部６６は、例えば、認証要求Ｉｎｆ１を認証装置５０に送信した後に、認証装置５０から認証応答Ｉｎｆ４を受信したときに、認証応答Ｉｎｆ４に含まれる認証要求の送信元の装置を示す装置ＩＤ情報と、記憶部６５から読み出した装置ＩＤ情報ID_{M1}～ID_{M4}の何れかとが一致するか否かを検出し、一致している場合には、正当な取り引きが行われていると判断し、不一致の場合には、不正な取り引きが行われたと判断して、その旨を受注者端末装置１５および認証装置５０の少なくとも一方に通知する。

【００２９】

〔受注者端末装置１５〕

図４に示すように、受注者端末装置１５は、サイバーモール(Cyber Moll)などに店舗を出している受注者３３が使用するサーバ装置であり、受信部７１、送信部７２、暗号化部７３、復号部７４、記憶部７５、制御部７６および署名検証部７７を有する。

受信部７１は、外部ネットワーク９を介して認証装置５０から情報あるいは要求を受信する。

送信部７２は、外部ネットワーク９を介して認証装置５０に情報あるいは要求を送信する。

また、受信部７１および送信部７２は、発注者端末装置１１からのアクセスに応じて、例えば、記憶部７５から読み出した受注者３３が提供する商品等の案内

情報を、ネットワークを介して、発注者端末装置１１に送信する。

暗号化部７３は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部７４は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部７５は、受注者３３が作成した秘密鍵$K_{33,S}$などを格納する。

制御部７６は、受注者端末装置１５内の各構成要素の処理を統括的に制御する。

署名検証部７７は、例えば、ネットワーク銀行４０の公開鍵$K_{40,P}$を用いて、認証装置５０が作成した署名情報の検証を行う。

【００３０】

〔認証装置５０〕

図５に示すように、認証装置５０は、受信部８１、送信部８２、暗号化部８３、復号部８４、記憶部８５、制御部８６、署名作成部８７および課金処理部８８を有する。

【００３１】

ここで、受信部８１が第２の発明の第２の受信手段に対応し、送信部８２が第２の発明の第２の送信手段に対応し、記憶部８５が第２の発明の第２の記憶手段に対応し、制御部８６が第２の発明の処理手段に対応している。

【００３２】

受信部８１は、外部ネットワーク９を介してホームゲートウェイ１２および受注者端末装置１５から情報あるいは要求を受信する。

送信部８２は、外部ネットワーク９を介してホームゲートウェイ１２および受注者端末装置１５に情報あるいは要求を送信する。

暗号化部８３は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部８４は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部８５は、発注者３１がネットワーク銀行４０と契約したときに、発注者３１の個人キー情報ｋ１と、個人ＩＤ情報ＩＤ１と、ホームゲートウェイ１２のアドレスとの対応表を記憶する。また、記憶部８５は、例えば、発注者３１および受注者３３がネットワーク銀行４０と契約をしたときに、発注者３１が作成した秘密鍵$K_{31,S}$に対応する公開鍵$K_{31,P}$、並びに受注者３３が作成した秘密鍵K

$33,S$に対応する公開鍵$K_{33,P}$などを格納する。

制御部８６は、認証装置５０内の各構成要素の処理を統括的に制御する。

署名作成部８７は、ネットワーク銀行４０の秘密鍵$K_{40,S}$を用いて署名情報の作成を行う。

課金処理部８８は、発注者３１による取り引きに関する認証に対しての課金処理を行う。

認証装置５０の各構成要素の詳細な処理については、後述する動作例で記載する。

【００３３】

以下、トランザクション認証システム１０１の動作例を説明する。

当該動作例では、図２に示す発注者３１が図２に示す端末装置11_1を操作して、受注者３３が提供する商品またはサービスの発注を行なう場合を説明する。

なお、当該動作例を開始する前提として、以下の手続および処理が行なわれている。

すなわち、発注者３１とネットワーク銀行４０との間で所定の契約が結ばれ、ネットワーク銀行４０は、発注者３１に対して、個人キー情報ｋ１および個人ＩＤ情報ＩＤ１を発行する。

ネットワーク銀行４０は、個人キー情報ｋ１と、個人ＩＤ情報ＩＤ１と、ホームゲートウェイ１２のアドレスとの対応表を図５に示す認証装置５０の記憶部８５に記憶する。ここで、個人キー情報ｋ１は、例えば、ネットワーク銀行４０と契約した契約者（発注者３１）の契約番号などの個人情報を示す識別子である。また、個人ＩＤ情報ＩＤ１は、発注者３１の銀行口座番号などの課金に係わる情報を示す識別子である。

【００３４】

また、ネットワーク銀行４０は、自らの秘密鍵$K_{40,S}$を図５に示す認証装置５０の記憶部８５に記憶すると共に、当該秘密鍵$K_{40,S}$に対応する公開鍵$K_{40,P}$をホームゲートウェイ１２および受注者端末装置１５に送信する。ホームゲートウェイ１２は、公開鍵$K_{40,P}$を図３に示す記憶部６５に記憶する。受注者端末装置１５は、公開鍵$K_{40,P}$を図４に示す記憶部７５に記憶する。

【００３５】

また、受注者３３とネットワーク銀行４０との間で所定の契約が結ばれ、ネットワーク銀行４０は、受注者３３に対して、個人キー情報Ｚおよび個人ＩＤ情報ＩＤ２を発行する。ネットワーク銀行４０は、個人キー情報Ｚおよび個人ＩＤ情報ＩＤ２の対応表を図５に示す認証装置５０の記憶部８５に記憶する。

【００３６】

また、ホームゲートウェイ１２の電源が投入されたときに電源がオンになっている端末装置11_1～11_4から内部ネットワーク１３を介してホームゲートウェイ１２が受信した装置ＩＤ情報ID_{M1}～ID_{M4}が、図３に示す記憶部６５に記憶される。

【００３７】

図６は、トランザクション認証システム１０１の動作例を説明するための図である。

ステップＳＴ１１：

図１に示す発注者３１は、例えばネットワーク上の商店である受注者３３に商品を発注する場合に、発注する商品名および数量などを示す発注情報ａ１と、発注者３１の個人キー情報ｋ１と、発注者３１の個人ＩＤ情報ＩＤ１とを、図示しない操作手段を操作して端末装置11_1に入力する。なお、発注情報ａ１には、受注者３３を特定する情報が含まれている。

端末装置11_1は、当該入力された発注情報ａ１と、発注者３１の個人キー情報ｋ１と、発注者３１の個人ＩＤ情報ＩＤ１と、内部メモリから読み出した装置ＩＤ情報ID_{M1}とを、内部ネットワーク１３を介して、ホームゲートウェイ１２に送信する。

【００３８】

ステップＳＴ１２：

図３に示すホームゲートウェイ１２は、発注情報ａ１と、個人キー情報ｋ１と、個人ＩＤ情報ＩＤ１と、装置ＩＤ情報ID_{M1}とを内部ネットワークＩ／Ｆ６２で受信し、これらの全体に対して暗号化部６３で暗号化を行う。

ホームゲートウェイ１２は、当該暗号化した情報を格納した認証要求Ｉｎｆ１

（本発明の要求）を、図３に示す外部ネットワークＩ／Ｆ６１から外部ネットワーク９を介して、図１に示すネットワーク銀行４０の認証装置５０に送信する。

【００３９】

ステップＳＴ１３：

図５に示す認証装置５０は、ホームゲートウェイ１２からの認証要求Ｉｎｆ１を受信部８１が受信すると、記憶部８５からネットワーク銀行４０の秘密鍵$K_{40,S}$を読み出し、復号部８４において、当該秘密鍵$K_{40,S}$を用いて認証要求Ｉｎｆ１を復号する。

次に、認証装置５０は、制御部８６の制御に基づいて、上記復号した認証要求Ｉｎｆ１に格納された発注情報ａ１および個人キー情報ｋ１を格納した情報Ｉｎｆ１’とについて、記憶部８５から読み出した自らの秘密鍵$K_{40,S}$を用いて署名情報Ａｕ１を作成する。

次に、認証装置５０は、情報Ｉｎｆ１’および署名情報Ａｕ１を格納した要求Ｉｎｆ２を生成する。

次に、暗号化部８３は、図５に示す記憶部８５から読み出した受注者３３の公開鍵$K_{33,P}$を用いて、上記生成した要求Ｉｎｆ２を暗号化した後に、送信部８２から、外部ネットワーク９を介して受注者端末装置１５に送信する。

【００４０】

ステップＳＴ１４：

受注者端末装置１５の復号部７４は、認証装置５０からの要求Ｉｎｆ２を受信部７１が受信すると、記憶部７５から読み出した自らの秘密鍵$K_{33,S}$を用いて、要求Ｉｎｆ２を復号する。

次に、受注者端末装置１５の署名検証部７７は、上記復号した要求Ｉｎｆ２に格納された署名情報Ａｕ１を、記憶部７５から読み出した認証装置５０の公開鍵$K_{40,P}$を用いて検証する。

【００４１】

受注者端末装置１５の制御部７６は、署名検証部が上記検証の結果、署名情報Ａｕ１の正当性が認証されると、要求Ｉｎｆ２に格納された情報Ｉｎｆ１’を図４に示す記憶部７５に記憶する。受注者３３は、情報Ｉｎｆ１’内の発注情報ａ

１に基づいて、発注者３１への商品等の発送予定などを示す受注確認情報ｃ１を生成する。

次に、制御部７６は、要求Ｉｎｆ２、受注確認情報ｃ１および自らの個人キー情報Ｚを格納した応答Ｉｎｆ３を生成する。

次に、受注者端末装置１５の送信部７２は、上記生成した応答Ｉｎｆ３を、記憶部７５から読み出したネットワーク銀行４０の公開鍵$K_{40,P}$を用いて暗号化部７３で暗号化した後に、送信部７２から、外部ネットワーク９を介して認証装置５０に送信する。

受注者３３は、例えば、要求Ｉｎｆ２に格納された情報Ｉｎｆ１’内の発注情報ａ１に基づいて、発注者３１が発注した商品等を発注者３１に発送したり、発注者３１が注文したサービスを発注者３１に提供する。

【００４２】

ステップＳＴ１５：

認証装置５０の復号部８４は、受注者端末装置１５からの応答Ｉｎｆ３を受信部８１が受信すると、記憶部８５から読み出した自らの秘密鍵$K_{40,S}$を用いて、Ｉｎｆ３を復号し、要求Ｉｎｆ１に格納された発注情報ａ１と、当該復号されたＩｎｆ３に格納された受注者３３の個人キー情報Ｚとを用いて、所定の取り引き履歴情報を作成し、これを記憶部８５に格納する。当該履歴情報は、ネットワーク銀行４０が、発注者３１に対して決済を行う際に用いられる。

また、認証装置５０の署名作成部８７は、ステップＳＴ１４で受信した応答Ｉｎｆ３について、自らの秘密鍵$K_{40,S}$を用いて署名情報Ａｕ２を作成する。

次に、認証装置５０の制御部８６は、応答Ｉｎｆ３および署名情報Ａｕ２を格納した認証応答Ｉｎｆ４を作成する。

次に、認証装置５０の暗号化部８３は、上記作成した認証応答Ｉｎｆ４を、記憶部８５から読み出した発注者３１の公開鍵$K_{31,P}$を用いて暗号化する。

そして、図５に示す記憶部８５に個人ＩＤ情報ＩＤ１と対応して記憶されているホームゲートウェイ１２のアドレスを用いて、送信部８２から外部ネットワーク９を介してホームゲートウェイ１２に当該暗号化した応答Ｉｎｆ４を送信する。

ホームゲートウェイ１２では、受信した認証応答Ｉｎｆ４を、図３示す記憶部６５から読み出した発注者３１の秘密鍵$K_{31,S}$を用いて復号部６４で復号する。

次に、ホームゲートウェイ１２の署名検証部６６は、当該復号した認証応答Ｉｎｆ４に格納された署名情報Ａｕ２を、記憶部６５から読み出したネットワーク銀行４０の公開鍵$K_{40,P}$を用いて検証すると共に、Ｉｎｆ４内の発注情報ａ１内に記述された装置ＩＤ情報$ＩＤ_{M1}$が図３に示す記憶部６５に記憶されている装置ＩＤ情報$ＩＤ_{M1}$～$ＩＤ_{M4}$の何れかと一致するか否かを判断する。当該動作例では、一致すると判断され、発注者３１と受注者３３との間の当該取り引きが正当に行われたことが確認される。

【００４３】

ステップＳＴ１６：

ホームゲートウェイ１２は、応答Ｉｎｆ４に含まれるＩｎｆ３を、内部ネットワーク１３を介して端末装置１１_{1}に送信する。

端末装置１１_{1}は、当該受信したＩｎｆ３に格納された受注確認情報ｃ１をディスプレイなどに表示する。

【００４４】

以下、発注者３１の個人ＩＤ１および個人キーｋ１を不正に取得した図１に示す不正者５５が自らの端末装置である不正者端末装置５６を用いて、認証装置５０に認証要求を送信した場合のトランザクション認証システム１０１の動作を説明する。

図７は、トランザクション認証システム１０１の当該動作を説明するための図である。

ステップＳＴ２１：

図１に示す不正者５５は、受注者３３に商品を発注する場合に、発注する商品名および数量などを示す発注情報ａ１と、不正に取得した発注者３１の個人キー情報ｋ１と、不正に取得した発注者３１の個人ＩＤ情報ＩＤ１とを、図示しない操作手段を操作して不正者端末装置５６に入力する。

不正者端末装置５６は、発注情報ａ１と、個人キー情報ｋ１と、個人ＩＤ情報ＩＤ１と、内部メモリから読み出した装置ＩＤ情報$ＩＤ_{M56}$を暗号化し、当該暗

号化した情報を格納した認証要求Ｉｎｆ１を、外部ネットワーク９を介して、図１に示すネットワーク銀行４０の認証装置５０に送信する。

図５に示す認証装置５０は、不正者端末装置５６からの認証要求Ｉｎｆ１を受信部８１が受信すると、当該認証要求Ｉｎｆ１について、前述したステップＳＴ１２と同様の処理を行なう。

【００４５】

ステップＳＴ２２：

ステップＳＴ２２の処理は、前述したステップＳＴ１３の処理と同じである。

【００４６】

ステップＳＴ２３：

ステップＳＴ２３の処理は、前述したステップＳＴ１４の処理と同じである。

【００４７】

ステップＳＴ２４：

ステップＳＴ２４の処理は、前述したステップＳＴ１５の処理と同じである。

【００４８】

ステップＳＴ２５：

ステップＳＴ２５の処理は、前述したステップＳＴ１６の処理と同じである。

【００４９】

このように、トランザクション認証システム１０１によれば、不正者５５が不正者端末装置５６を用いて、認証要求Ｉｎｆ１を認証装置５０に送信した場合でも、その応答である認証応答Ｉｎｆ４は、認証装置５０の記憶部８５に個人ＩＤ情報ＩＤ１と対応して記憶されているホームゲートウェイ１２のアドレスに基づいて、ホームゲートウェイ１２に送信される。

これにより、ホームゲートウェイ１２において、認証応答Ｉｎｆ４に含まれる装置ＩＤ情報$ＩＤ_{M56}$が、図３に示す記憶部６５に記憶されている装置ＩＤ情報$ＩＤ_{M1}$～$ＩＤ_{M4}$と一致しないと判断され、発注者３１の個人ＩＤ情報ＩＤ１を用いた不正な認証要求が行なわれたことを検出できる。

そのため、トランザクション認証システム１０１によれば、他人の個人ＩＤ情報を用いた不正な取り引きを効果的に抑制できる。

【００５０】

上述したように、トランザクション認証システム１０１によれば、電子商取引の信頼性を向上でき、当該認証機関と契約する契約者（取り引き者）の数を増やし、各契約者に課す会費などを費用を低額にでき、電子商取引をさらに普及させることが可能になる。

【００５１】

また、トランザクション認証システム１０１によれば、例えば、図１および図２に示す端末装置11_1からの要求に応じて認証要求Ｉｎｆ１を認証装置５０に送信した後に、端末装置11_1が故障した場合でも、当該認証要求Ｉｎｆ１に応じた認証応答Ｉｎｆ４に応じた処理を適切に行うことができる。

【００５２】

また、トランザクション認証システム１０１によれば、外部ネットワーク９を介した通信に伴うセキュリティに関する機能をホームゲートウェイ１２に持たせることで、端末装置11_1～11_4に備えるセキュリティ機能のレベルを下げることができ、端末装置11_1～11_4の構成を簡単かつ安価にできる。

【００５３】

本発明は上述した実施形態に限定されない。

例えば、上述した実施形態では、本発明の第２の通信装置として認証処理を行う認証装置５０を例示したが、第２の通信装置が行う処理はその他、課金処理などであってもよい。

また、上述した実施形態では、ネットワーク銀行４０が、認証装置５０を用いて、トランザクション（取り引き）の認証業務を行う場合を例示したが、ネットワーク銀行４０とは別の機関が、認証装置５０を用いてトランザクションの認証業務を行うようにしてもよい。

【００５４】

また、上述した実施形態では、端末装置11_1～11_4の装置ＩＤ情報を認証装置５０に送信した場合を例示したが、ホームゲートウェイ１２の装置ＩＤ情報を認証装置５０に送信するようにしてもよい。

【００５５】

【発明の効果】

以上説明したように、本発明によれば、不正に取得した他人の識別情報（個人ＩＤ情報）に基づいて不正な認証手続が行われることを回避する通信制御装置、通信システムおよびその方法を提供できる。

また、本発明によれば、複数の通信装置を用いてネットワークを介した電子商取引などを行う場合に、当該電子商取引に必要な機能の割り当て、並びに通信履歴の管理を効率的に行うことができる通信制御装置、通信システムおよびその方法を提供できる。

【図面の簡単な説明】

【図１】

図１は、本発明の実施形態のトランザクション認証システムの全体構成図である。

【図２】

図２は、図１に示すホームネットワークシステムを説明するための図である。

【図３】

図３は、図２に示すホームゲートウェイの構成図である。

【図４】

図４は、図１に示す受注者端末装置の構成図である。

【図５】

図５は、図１に示す認証装置の構成図である。

【図６】

図６は、正当者が認証要求を出した場合の図１に示すトランザクション認証システムの動作例を説明するための情報の流れを示す図である。

【図７】

図７は、不正者が認証要求を出した場合の図１に示すトランザクション認証システムの動作例を説明するための情報の流れを示す図である。

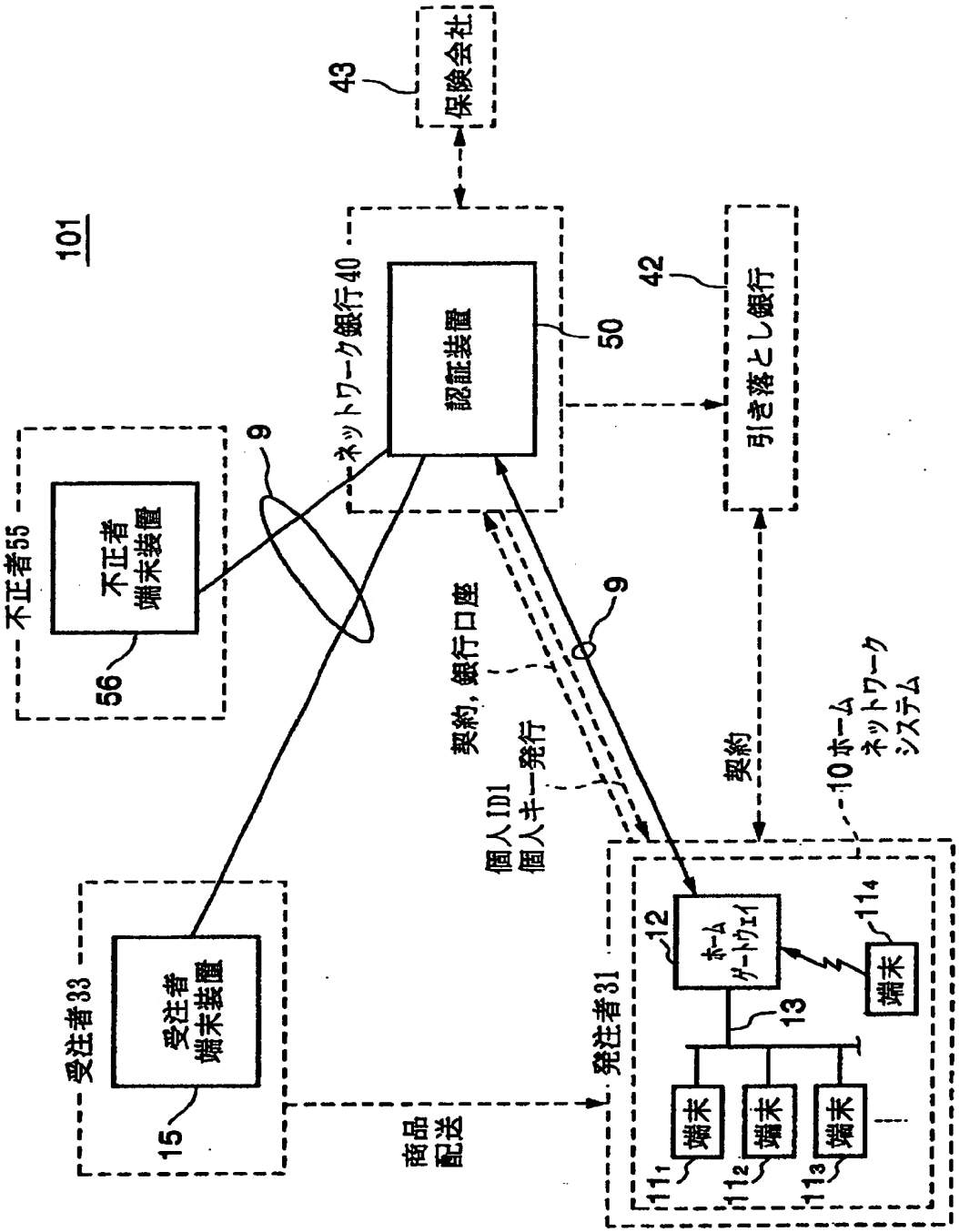
【符号の説明】

１…トランザクション認証システム、１１…発注者端末装置、１５…受注者端末装置、３１…発注者、３３…受注者、４０…ネットワーク銀行、５０…認証装

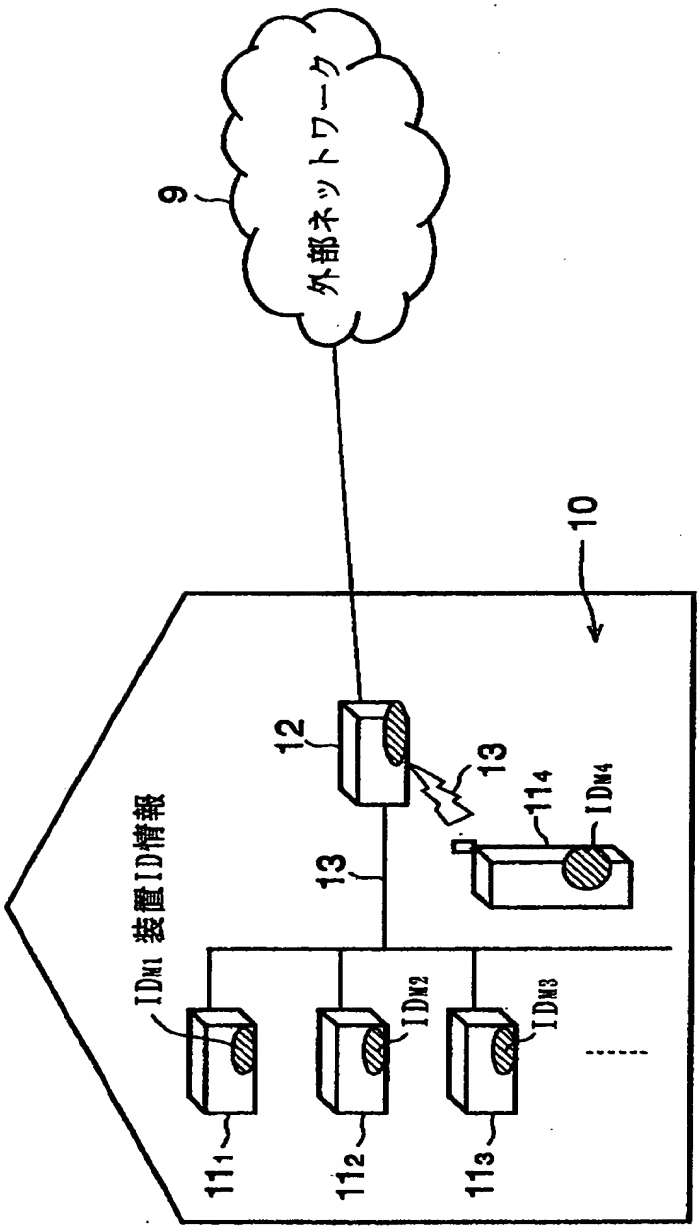
置、６１…外部ネットワークＩ／Ｆ、６２…内部ネットワークＩ／Ｆ、７１，８１…受信部、７２，８２…送信部、６３，７３，８３…暗号化部、６４，７４，８４…復号部、６５，７５，８５…記憶部、６６，７６，８６…制御部、６７，７７…署名検証部、，８７…署名作成部、８８…課金処理部、ａ１…発注情報、ｋ１…発注者３１の個人キー情報ｋ１、ＩＤ１…発注者３１の個人ＩＤ情報、ID_{M1}，ID_{M2}，ID_{M3}，ID_{M4}，ID_{M56}…装置ＩＤ情報、Ａｕ１，Ａｕ２…認証装置の署名情報、Ｚ…受注者の個人キー情報、Ｉｎｆ１…認証要求、Ｉｎｆ４…認証応答

【書類名】　図面

【図１】

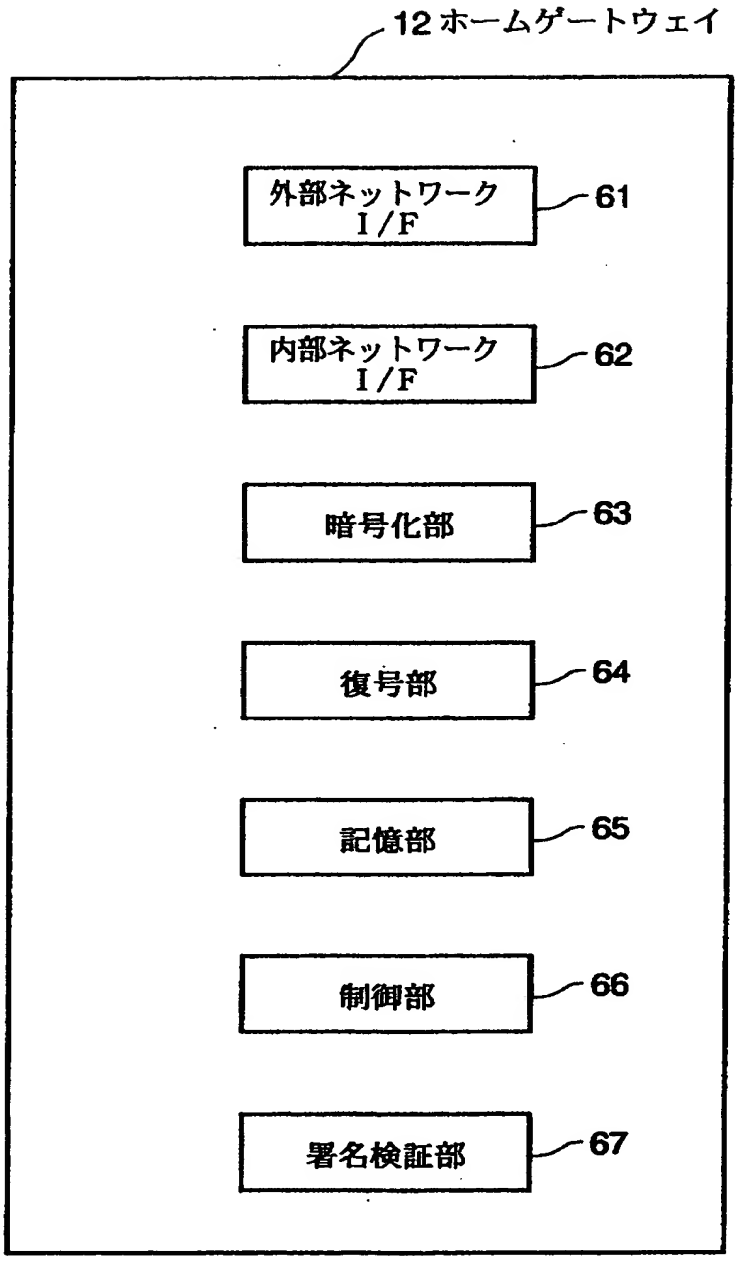

101
43
保険会社
ネットワーク銀行40
認証装置
50
42
引き落とし銀行
不正者55
不正者端末装置
56
9
契約，銀行口座
個人ID1
個人キー発行
9
契約
10 ホームネットワークシステム
受注者33
受注者端末装置
15
商品配送
発注者31
12
ホームゲートウェイ
114
端末
13
端末
端末
端末
111
112
113

【図２】

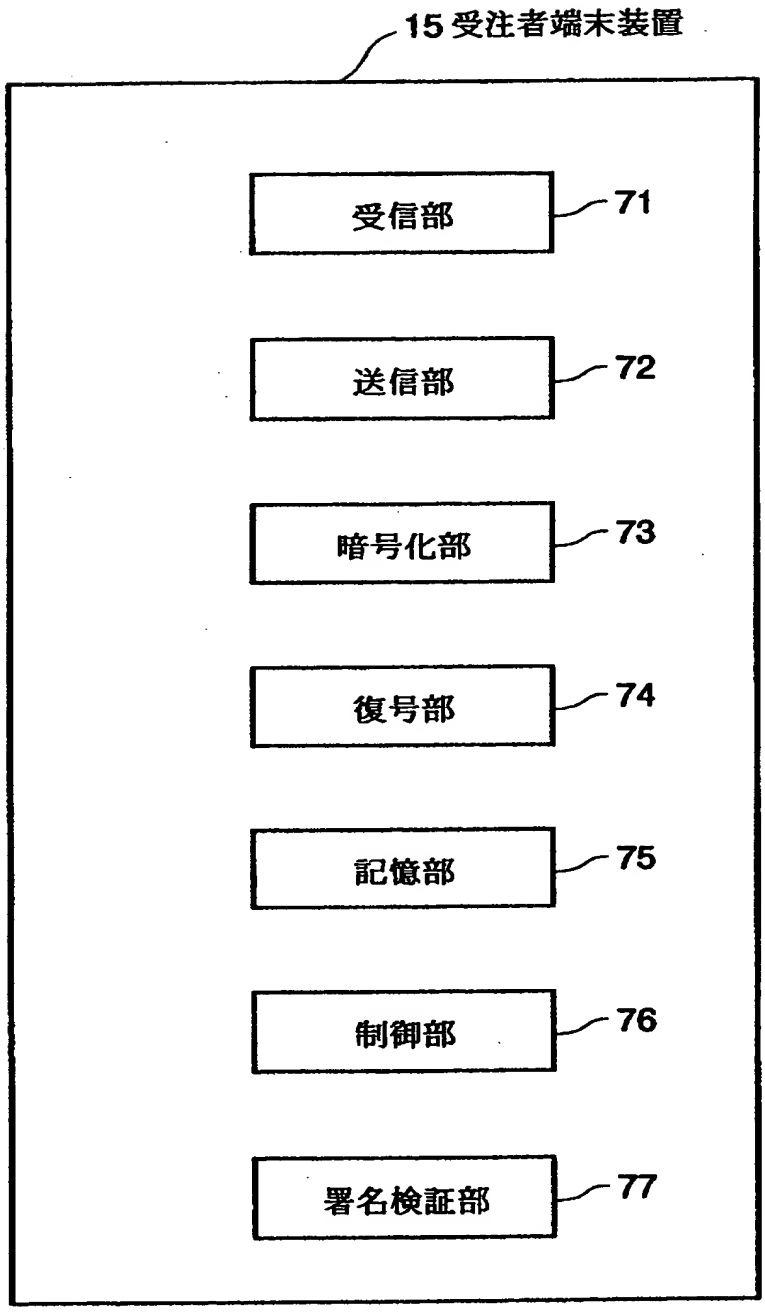


出証特２００１－３０１５１６４

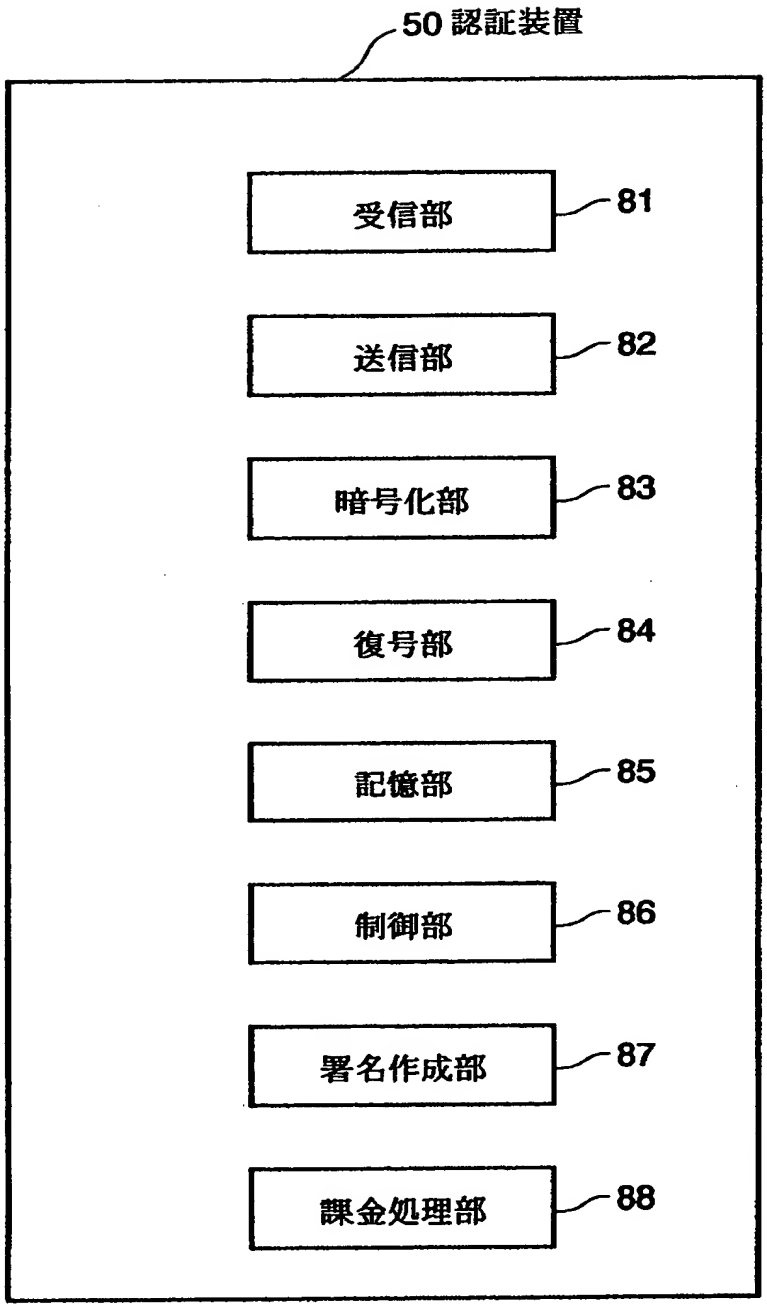
【図３】


12 ホームゲートウェイ
外部ネットワーク I/F
61
内部ネットワーク I/F
62
暗号化部
63
復号部
64
記憶部
65
制御部
66
署名検証部
67

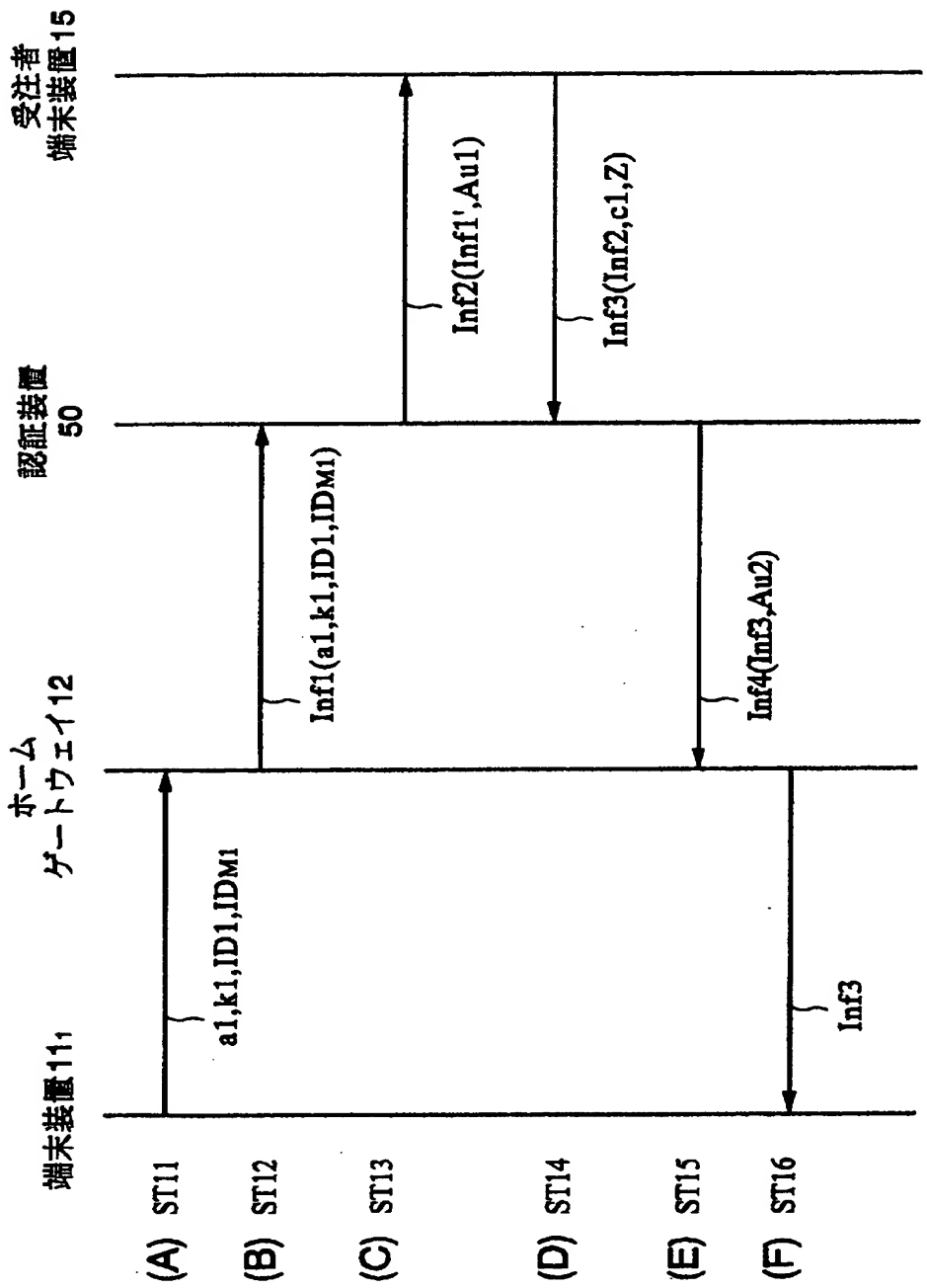
【図４】



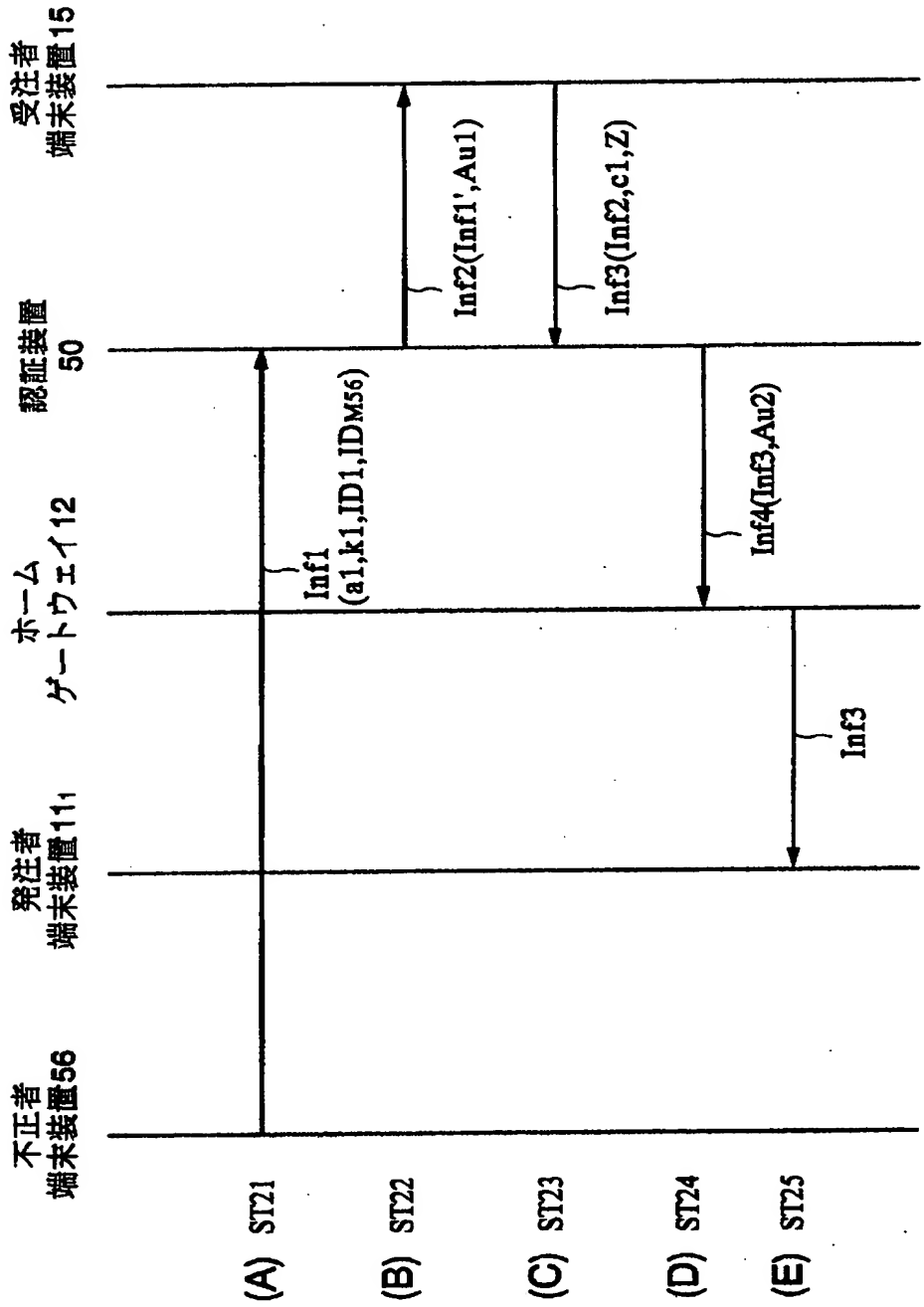
【図５】


50 認証装置
受信部
81
送信部
82
暗号化部
83
復号部
84
記憶部
85
制御部
86
署名作成部
87
課金処理部
88

【図６】


端末装置11₁
ホームゲートウェイ12
認証装置50
受注者端末装置15
a1,k1,ID1,IDM1
Inf1(a1,k1,ID1,IDM1)
Inf2(Inf1',Au1)
Inf3(Inf2,c1,Z)
Inf4(Inf3,Au2)
Inf3
(A) ST11
(B) ST12
(C) ST13
(D) ST14
(E) ST15
(F) ST16

【図７】


受注者
端末装置15
認証装置
50
ホーム
ゲートウェイ12
発注者
端末装置11₁
不正者
端末装置56
Inf2(Inf1',Au1)
Inf3(Inf2,c1,Z)
Inf1
(a1,k1,ID1,IDM56)
Inf4(Inf3,Au2)
Inf3
(A) ST21
(B) ST22
(C) ST23
(D) ST24
(E) ST25

【書類名】　　要約書

【要約】

【課題】　不正に取得した他人の個人ＩＤ情報に基づいて不正な手続が行われることを回避する通信制御装置を提供する。

【解決手段】　ホームゲートウェイ１２は、端末装置11_1～11_4を識別するための装置識別情報ID_{M1}～ID_{M4}を記憶し、端末装置１１からの要求に応じて、当該端末装置に対応する装置識別情報を含む要求を認証装置５０に送信し、前記要求の送信元の装置を識別するための装置識別情報を含む応答を認証装置５０から受信し、当該応答に含まれる装置識別情報と、前記記憶している装置識別情報とが一致するか否かに基づいて、前記受信した応答に対応した前記要求が、正当な端末装置１１によるものであるかを判断する。

【選択図】　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００２１８５〕

１．変更年月日　　１９９０年　８月３０日
　［変更理由］　　新規登録
　　住　所　　東京都品川区北品川６丁目７番３５号
　　氏　名　　ソニー株式会社